Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (original) A cryptographic communication method wherein when different encryption algorithms are operated at a transmission side and a reception side, the transmission side encrypts an encryption algorithm operated at the transmission side with an encryption algorithm operated at the reception side and transmits the encrypted algorithm to the reception side.

2. (original) A cryptographic communication method wherein information on an encryption algorithm operated at a transmission side and information on an encryption algorithm operated at a reception side are obtained from the transmission side and when different encryption algorithms are operated at the transmission side and the reception side, an encryption algorithm operated at the transmission side is encrypted with an encryption algorithm operated at the reception side and transmitted to the reception side.

3. (currently amended) A cryptographic communication method as claimed in claim 2 wherein signature data produced based on a public key preliminarily allocated to the transmission side is supplied to the reception side with said [encrypted] encryption

algorithm operated at the transmission side with the encryption algorithm operated at the reception side.

4. (currently amended) A cryptographic communication method as claimed in claim 2 wherein signature data produced based on a public key preliminarily allocated to the transmission side is supplied to the transmission side together with said [encrypted] encryption algorithm operated at the transmission side encrypted with the encryption algorithm operated at the reception side and transmitted to the reception side.

5. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between] [the] user identifiers indicating [the] users and [an] their corresponding encryption algorithms [operated by the user is] are preliminarily described, [about each user and then retrieving] so as to obtain an [the] encryption algorithm operated by the user of the transmission side and [the] an encryption algorithm operated by the user of the reception side,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, data indicating [the] said encryption algorithm operated by the user of the transmission side is encrypted with [the] said encryption algorithm operated by the user

of the reception side and transmitted to the user of the reception side.

6. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side;

querying a data base in which [a correspondence between] user identifiers indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described [about each user] so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, data indicating [the] said encryption algorithm operated by the user of the transmission side and an encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of [the] said encryption algorithm operated by the user of the transmission side is encrypted with [the] said encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

7. (currently amended) An encryption algorithm sharing management

method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user of the transmission side identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between] user identifiers indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described [about each user] so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and [the] an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and [data obtained by encrypting the] said encryption algorithm operated by the user of the transmission side is encrypted with [the] said encryption algorithm operated by the user of the reception side and [signature data produced for the encryption key operated by the user of the reception side] are transmitted to the user of the reception side with signature data produced for the encryption key operated by the user of the reception side.

8. (currently amended) An encryption algorithm sharing management method for sharing the encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between the] user identifiers indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described [about each user] so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data indicating [the] said encryption algorithm operated by the user of the transmission side and an encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of [the] said encryption algorithm operated by the user of the transmission side is encrypted with [the] said encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side with [the] signature data produced [corresponding to] for the encryption key operated by the user of the reception side.

9. (currently amended) A [N]network communication system composed by connecting a plurality of users, comprising at least [an] one encryption key management station to be connected from a user of a transmission side,

said encryption key management station obtaining, from the user of the transmission side, information indicating an encryption algorithm operated by the user of the transmission side and information indicating [the] an encryption algorithm operated by [the] a user of [the] a reception side and if different encryption algorithms are operated by [users] the user of the transmission side and [a] the user of the reception side, encrypting the encryption algorithm operated by the user of the transmission side with [an] the encryption algorithm operated by the user of the reception side and transmitting it to the user of the reception side.

10. (currently amended) A [N] network communication system composed by connecting a plurality of users, comprising at least [an] one encryption key management station to be connected from a user of a transmission side,

said encryption key management station comprising a data base in which a correspondence between a user identifier indicating a user and an encryption algorithm operated by [the] said user is preliminarily described about each user;

wherein when a communication is carried out from the user of the transmission side to a user of a reception side, a user identifier indicating the user of the transmission side and a [reception side] user identifier indicating a user of a reception side are obtained from the user of the transmission side and said data base is queried with the obtained identifiers as a key so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side, and

if the encryption algorithm operated by the user of the transmission side is

different from the encryption algorithm operated by the user of the reception side, the encryption algorithm operated by the user of the transmission side is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

11. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between the] user identifiers indicating [the] users and [an] their corresponding encryption algorithms, [operated by the user] [is] are preliminarily described [about each user] so as to [retrieve] obtain an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side; [and]

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, data indicating [the] said encryption algorithm operated by the user of the [transmission] reception side is encrypted with [the] said encryption algorithm operated by the user of the [reception] transmission side and transmitted to the user of the [reception] transmission side.

12. (currently amended) An encryption algorithm sharing management

method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; [and]

querying a data base in which [a correspondence between the] user identifiers indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described [about each user] so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and [the] an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, data indicating [the] said encryption algorithm operated by the user of the [transmission] reception side and [the] an encryption key produced based on the encryption key operated by the user of the [reception] transmission side corresponding to a key length of [the] said encryption algorithm operated by the user of the reception side is encrypted with [the] said encryption algorithm operated by the user of the [reception] transmission side and transmitted to the user of the [reception] transmission side.

13. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user

of the transmission side and a user identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between the] user identifiers indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described about each user so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and [the] an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the [transmission] reception side is transmitted to the user of the [transmission] reception side and [the] said encryption algorithm operated by the user of [transmission] the reception side is encrypted with [the] said encryption algorithm operated by the user of the [reception] transmission side and transmitted to the user of the [reception] transmission side with the signature data produced for the encryption key operated by the user of [reception] the transmission side.

14. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side; and

querying a data base in which [a correspondence between the] user identifiers

indicating [the] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described about each user so as to obtain [the] an encryption algorithm operated by the user of the transmission side and an encryption key thereof and [the] an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if [the] said encryption algorithm operated by the user of the transmission side is different from [the] said encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the [transmission] reception side is transmitted to the user of the [transmission] reception side and data indicating [the] said encryption algorithm operated by the user of the [transmission] reception side and [the] an encryption key produced based on the encryption key operated by the user of the [reception] transmission side corresponding to a key length of [the] said encryption algorithm operated by the user of the reception side is encrypted with [the] said encryption algorithm operated by the user of the [reception] transmission side and transmitted to the user of the [reception] transmission side with signature data produced [corresponding] for to the encryption key operated by the user of the [reception] transmission side.

15. (currently amended) A [N] network communication system composed by connecting a plurality of users, comprising at least [an] one encryption key management station to be connected from a user of a transmission side,

said encryption key management station obtaining, from the user of the transmission side, information indicating an encryption algorithm operated by the user of

the transmission side and information indicating an encryption algorithm operated by a user of a reception side, and [when] if different encryption algorithms are operated by the user of the transmission side and the user of the reception side, encrypting the encryption algorithm operated by the user of the [transmission] reception side with the encryption algorithm operated by the user of the [reception] transmission side and [transmitted] transmitting it to the user of the [reception] transmission side.

16. (currently amended) A [N] network communication system composed by connecting a plurality of users, comprising at least [an] one encryption key management station to be connected from a user of a transmission side,

said encryption key management station comprising a data base in which a correspondence between a user identifier indicating a user and an encryption algorithm operated by [the] said user is preliminarily described about each user;

wherein when a communication is carried out from the user of the transmission side to a user of a reception side, a user identifier indicating the user of the transmission side and a [reception side] user identifier indicating a user of a reception side are obtained from the user of the transmission side, and said data base is queried with the obtained identifiers as a key so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side, and

if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, the encryption algorithm operated by user of [transmission] the reception side is encrypted

with the encryption algorithm operated by the user of the [reception] transmission side and transmitted to the user of the [reception] transmission side.

17. (currently amended) A cryptographic communication method wherein if different encryption algorithms are operated by a transmission side and a reception side, an encryption algorithm operated by the reception side is encrypted with an encryption algorithm operated by the transmission side and transmitted to the [reception] transmission side.

18. (original) A cryptographic communication method wherein information indicating an encryption algorithm operated by a transmission side and information indicating an encryption algorithm operated by a reception side are obtained from the transmission side and when different encryption algorithms are operated by the transmission side and the reception side, the encryption algorithm operated by the reception side is encrypted with the encryption algorithm operated by the transmission side and transmitted to the transmission side.

19. (currently amended) A cryptographic communication method as claimed in claim 18 wherein signature data produced based on a public key preliminarily allocated to the reception side is supplied to the transmission side with the [encrypted] encryption algorithm operated by the reception side encrypted with the encryption algorithm operated by the transmission side.

20. (currently amended) An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user of the transmission side and a user identifier indicating a user of a reception side;

querying a data base in which [a correspondence between the] user identifiers indicating [the] users and [an] corresponding encryption algorithms [operable by the user] [is] are preliminarily described [about each user] so as to obtain an encryption algorithm operable by the user of the transmission side and an encryption algorithm operable by the user of the reception side;

determining whether or not there is an encryption algorithm operable by the user of the transmission side and the user of the reception side commonly; and

if the commonly operable encryption algorithm exists, [it is notified] the user of the transmission side is notified that cryptographic communication at the user of the transmission side and the user of the reception side is enabled.

21. (currently amended) An encryption algorithm sharing management method as claimed in claim 20 wherein:

if the commonly operable encryption algorithm exists, information indicating the commonly operable encryption algorithm is transmitted to the user of the transmission side and

if the commonly operable encryption algorithm does not exists, [it is notified] the user of the reception side is notified that cryptographic communication at the user of the

transmission side and the user of the reception side is disabled.

22. (currently amended) An encryption algorithm conversion method for converting a[n operating] first encryption algorithm to [other] a second encryption algorithm comprising:

querying a data base in which [a correspondence between a] user identifiers indicating [a] users, [an] corresponding encryption algorithms [operated by the user] and [an] encryption keys thereof, [is] are preliminarily described [with] for a user, whose encryption algorithm is to be converted [with] as a key, so as to obtain a first encryption algorithm operated by the user whose encryption algorithm is to be converted and a first encryption key thereof; and

with a first management secret key preliminarily allocated for management and [operated on] applied to the firs encryption algorithm, supplying first and second signature data [written in] for the first encryption key and a second encryption key[s], public key data obtained by encrypting a second public key corresponding to a second management secret key [operated on] applied to [the] a second encryption algorithm preliminarily allocated for management with the first encryption algorithm, [a] the second encryption algorithm encrypted with the first encryption algorithm and signature data produced based on the second management secret key to the user whose encryption algorithm is to be converted.